AMEAÇAS E VULNERABILIDADES EM SISTEMAS E REDES: DESAFIOS ATUAIS E ESTRATÉGIAS DE MITIGAÇÃO

João Vitor Tibes de Campos[1], Willian Ferreira[2], Kalil Massignani da Rosa[3], Matheus Henrique Friebel[4], Leandro Otavio Cordova Vieira[5]

1. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
2. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
3. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
4. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
5. Docente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC

Autor correspondente: João Vitor Tibes de Campos, joaovcampos023@gmail.com

Área: Ciências Exatas e Tecnológicas

Introdução: Este artigo apresenta uma análise abrangente das principais ameaças cibernéticas contemporâneas, incluindo malware, phishing, ransomware e vulnerabilidades em redes Wi-Fi, com base em pesquisas recentes (2023-2024), através de revisões e análises nos frameworks como NIST Cybersecurity Framework e MITRE ATT&CK, podemos estar propondo um conjunto integrado de soluções para a mitigação de riscos. Os resultados de pesquisa e estudo demonstram que a combinação de tecnologias avançadas, como SIEM e EDR, gestão proativa de vulnerabilidades e capacitação humana pode reduzir em até 75% os incidentes de segurança. O estudo destaca a eficácia de medidas específicas, como a implementação de WPA3 para redes Wi-Fi, treinamentos anti-phishing e backups isolados. **Objetivo:** Analisar as principais ameaças cibernéticas contemporâneas e propor um conjunto integrado de soluções práticas e baseadas em evidências para a sua mitigação, com foco em tecnologias avançadas, gestão de vulnerabilidades e capacitação humana. **Método:** Utilizou-se uma revisão sistemática de 25 fontes (artigos, relatórios e normas de 2019–2023) com descritores como "cybersecurity threats" e "ransomware mitigation", aplicando critérios de inclusão/exclusão baseados em atualidade e validação empírica. Complementou-se com análise comparativa de 10 ferramentas de segurança (avaliadas por taxa de detecção, custo e facilidade de implementação) e simulações em ambiente controlado para testar eficácia de EDR, treinamentos anti-phishing e WPA3. O estudo não envolveu participantes humanos ou animais, dispensando aprovação ética. **Resultados:** O estudo demonstrou reduções significativas em três métricas críticas após a implementação das estratégias propostas: Ataques de Phishing: Redução de 60% (42 para 17 incidentes/mês). Ransomware: Redução de 100% (5 para 0 ataques/ano). Tempo de Detecção (MDTT): Queda de 87% (72 para 9 horas). Os resultados, obtidos em ambiente controlado, confirmaram a eficácia da combinação de tecnologias (EDR, SIEM, WPA3), gestão de vulnerabilidades e treinamentos. Limitações incluem a variação potencial em cenários reais e o número limitado de ferramentas testadas. **Conclusão:** Este estudo apresentou uma análise das principais ameaças cibernéticas contemporâneas, como phishing, ransomware e vulnerabilidades em redes sem fio, propondo soluções práticas fundamentadas em evidências recentes (2023–2024). A metodologia integrada, que combinou revisão bibliográfica, análise comparativa e experimentação controlada, evidenciou a eficácia da combinação entre tecnologias avançadas (EDR, SIEM, WPA3) e processos estruturados, aliados à capacitação contínua dos usuários.

Palavras-chave: Cibersegurança; Mitigação de Ameaças; Resiliência Digital.